

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

JOHN GRUBB,)
)
Plaintiff,) Case No. 09-cv-2255
)
v.) Judge Robert M. Dow, Jr.
)
BOARD OF TRUSTEES OF THE)
UNIVERSITY OF ILLINOIS,)
)
Defendant.)

MEMORANDUM OPINION AND ORDER

Plaintiff, John Grubb (“Grubb”), filed this lawsuit under the Computer Fraud and Abuse Act (18 U.S.C. § 1030) (“CFAA” or the “Act”). Among other things, the CFAA makes it illegal to intentionally engage in unauthorized access of a “protected computer,” where the unauthorized access causes “damage and loss.” 18 U.S.C. §§ 1030(a)(5)(B)-(C). “Damage” and “loss” are terms of art under the Act. *Id.* § 1030(d). Violators of the CFAA face potential criminal liability and may also be subject to civil suit: a person who suffers damage or loss as a result of a CFAA violation may obtain money damages, equitable relief, or both. *Id.* § 1303(g). Grubb maintains that Defendant, the Board of Trustees of the University of Illinois (“UIC”), violated the CFAA when it “hacked” into Grubb’s computer to remove software. The Court has subject-matter jurisdiction pursuant to 28 U.S.C. § 1331.

Before the Court is UIC’s motion for sanctions for spoliation of evidence [14], in which Defendant contends that Plaintiff first sullied and then “wiped” the computer whose forensic fingerprints are at the heart of the case. For the reasons set forth below, Defendant’s motion is denied.

I. Background

The case is brought under the CFAA, but the hard feelings between the parties start with UIC’s decision to end its employment relationship with Grubb. Grubb was a clinical professor at the UIC College of Dentistry from January 2007 to August 2008. Compl. ¶ 6. For reasons that do not bear on the CFAA claim, UIC ended its relationship with Grubb prior to the three-year period of employment that the parties originally had anticipated. See generally Compl. ¶¶ 9-31.

On July 18, 2008, after Grubb was placed on administrative duties and forbidden from having contact with orthodontic residents (Compl. ¶ 27), a person from UIC’s information technology department named Martin came to Grubb’s office. Grubb was in a meeting with another faculty member at the time. Martin told Grubb that he had been ordered to remove certain UIC software from Grubb’s laptop computer. Compl. ¶ 31. Grubb advised Martin that he was unavailable to supervise the work—which Grubb aimed to do because the laptop had confidential information on it—but that Martin could return on July 21 to remove the UIC software. Compl. ¶¶ 35, 41. However, when Grubb returned from lunch on July 18, he discovered that UIC’s information technology department had accessed the laptop computer and removed the UIC software. According to the complaint, the “hacking” caused at least \$5,000 in damages; according to Grubb’s deposition testimony the damage was far more severe, totaling nearly \$1 million. Compare Compl. ¶ 45, with Grubb Dep. at 201. When Grubb confronted UIC’s IT department about the breach, a worker responded, “[W]e’re asked to do a lot of shitty things around here.” Grubb Dep. at 101.

The laptop computer was owned not by Grubb but by the American Board of Orthodontics (“ABO”). Compl. ¶ 32. According to Grubb, the computer contained personal and sensitive information, as well as testing data and private patient information. Compl. ¶¶ 33, 40.

After the July 18 incident, Grubb informed ABO about the incident and raised the concern that information on the computer may have been compromised. Although the record is a bit murky on this point, it appears that counsel for ABO recommended forming a committee to handle any dispute with UIC. It also appears that Grubb's computer expertise, like most people, falls somewhere in that broad swath between technophobe and technophile: "I don't know anything about computers other than that I turn them on and I hope they work, and I'm very astute at using Adobe Photoshop, PowerPoint those kinds of issues." Grubb Dep. at 183.

On August 18, 2008, a lawyer from the firm Sidley Austin LLP, which represented ABO, sent Grubb an e-mail directing him to stop using the laptop computer:

I have been advised by our [sic] IT security folks that, if you have been using the computer, it is imperative that you stop using it as soon as possible. The more it is used after the unauthorized access, the harder it will be for us to document what materials were accessed. We are trying to identify a local expert to check the access history on the computer and I will let you know as soon as we have made that determination.

Def. Mem., Ex. F (Lynn D. Fleisher e-mail). Grubb, apparently unsatisfied with the expertise of lawyers, asked ABO's IT specialist, McEvoy, for his thoughts on what the lawyer had written. Grubbs told McEvoy that between the July 18 incident and the August 18 e-mail from the lawyer, he had frequently used the computer. McEvoy indicated that if Grubb had "used the computer a lot it would be very difficult to find out what was accessed." Grubb Dep. at 179. In addition, McEvoy "questioned [the lawyer's] IT skills as to make that judgment because that's what he [McEvoy] does for a living." Grubb Dep. at 181. McEvoy further indicated that it would be "impossible" to determine what UIC had accessed on the computer based on the total amount of Grubb's usage to that point. McEvoy recommended that Grubb continue to use the computer. Grubb Dep. at 181-82.

In November 2008, ABO gave Grubb a new computer. Grubb returned the old computer to ABO. At that time, ABO IT specialist McEvoy transferred material from the old computer to the new computer. He then “mirrored” the hard drive on the old computer and kept that mirror “for about two to three weeks,” before wiping the hard drive of the old computer and deleting the mirrored image of that old hard drive. Grubb Dep. at 23.

II. Analysis

UIC’s motion for sanctions for spoliation of evidence [14] contends that Grubb “has rendered it impossible for [UIC] to prove the content or condition of the laptop computer on the date of Defendant’s access; what was accessed by Defendant; and whether any data or information on the laptop computer was impaired by Defendant’s access on July 18, 2008.” Def. Mem. at 2. Spoliation of evidence occurs where a party “destroys evidence relevant to an issue in the case.” *Smith v. United States*, 293 F.3d 984, 988 (7th Cir. 2002). UIC asks that the case be dismissed or, alternatively, that the Court deem admitted that UIC did not access, obtain, alter, or destroy Grubb’s laptop or its contents.¹

UIC’s motion raises a serious issue, because the judicial system is premised on the honesty and good faith efforts of the parties involved. See *Quela v. Payco-Gen. Am. Credits, Inc.*, 2000 WL 656681, at *7 (N.D. Ill. May 18, 2000). Where honesty is replaced with falsehood, a party’s right to litigate before this Court comes into question. *Id.*; see also *Krumwiede v. Brighton Assocs., LLC*, 2006 WL 1308629, at *8-11 (N.D. Ill. May 8, 2006). The Seventh Circuit has warned that “[l]awyers and litigants who decide they will play by rules of

¹ Given UIC’s admission in its answer that Martin removed the software from Grubb’s computer, the requested admission regarding access is off the table.

their own invention will find that the game cannot be won.” *Nw. Nat'l Ins. Co. v. Baltes*, 15 F.3d 660, 663 (7th Cir. 1994).

A. Legal Standard

Before a Court may impose sanctions for the destruction of evidence, the party moving for sanctions must make a showing that destruction of materials occurred in bad faith. *Trask-Morton v. Motel 6 Operating L.P.*, 534 F.3d 672, 681 (7th Cir. 2008). Bad faith generally means that the destruction occurred “for the purpose of hiding adverse information.” *Mathis v. John Morden Buick, Inc.*, 136 F.3d 1153, 1155 (7th Cir. 1998); see also *Marrocco v. Gen. Motors Corp.*, 966 F.2d 220, 224 (7th Cir. 1992) (bad faith is “conduct which is either intentional or in reckless disregard of a party’s obligations to comply with a court order”). In addition, where destruction occurs prior to litigation, it must be shown that the non-moving party had “a duty to preserve evidence because it knew, or should have known, that litigation was imminent.” *Trask-Morton*, 534 F.3d at 681.

Where the required showings have been made, the Court has the power to enter a default judgment or dismiss a case—or to impose a less severe sanction—under the Court’s inherent authority or pursuant to Rule 37 of the Federal Rules of Civil Procedure. See *Grochocinski v. Schlossberg*, 402 B.R. 825, 842-43 (N.D. Ill. 2009) (a party’s destruction of, and failure to preserve, evidence is sufficient evidence of bad faith to warrant imposition of default judgment); *Krumwiede*, 2006 WL 1308629, at *8 (default judgment as a sanction even where evidence was destroyed prior to commencing litigation); *Quela*, 2000 WL 656681, at *6 (entering default judgment where a defendant falsified evidence and testimony to influence case outcome) (citing *Diettrich v. Nw. Airlines, Inc.*, 168 F.3d 961, 964 (7th Cir. 1999)); *Ciba Specialty Chems., Corp. v. Zinkan Enters., Inc.*, 2003 WL 22309275, at *4 (S.D. Ohio July 29, 2003) (ordering dismissal

of declaratory judgment claims and striking of affirmative defenses in response to serious abuses).

Default judgment or dismissal is appropriate where a lesser sanction under the circumstances would unfairly minimize the seriousness of the misconduct and fail sufficiently to deter such misconduct by others in the future. See *REP MCR Realty, L.L.C. v. Lynch*, 363 F. Supp. 2d 984, 997-98 (N.D. Ill. 2005); see also *Marrocco*, 966 F.2d at 223-24. Litigants cannot be permitted to say “‘oops, you’ve caught me’, and thereafter be allowed to continue to play the game * * *.” *Dotson v. Bravo*, 202 F.R.D. 559, 573 (N.D. Ill. 2001), *aff’d*, 321 F.3d 663 (7th Cir. 2003). Nonetheless, when considering the extreme sanction of dismissing a case with prejudice, the Court is mindful of the admonition that such a step “must be infrequently resorted to by district courts.” *Schilling v. Walworth County Park and Planning Commission*, 805 F.2d 272, 275 (7th Cir. 1986); *United States v. Golden Elevator, Inc.*, 27 F.3d 301, 303 (7th Cir. 1994). The organizing principle is that the sanction should be proportionate to the wrong. See, e.g., *Collins v. Illinois*, 554 F.3d 693, 698 (7th Cir. 2009) (per curiam).

As to UIC’s burden in supporting its sanctions motion, Grubb asserts that a “clear and convincing” standard must be met to support an outright dismissal. There is case law to that effect, although a more recent Seventh Circuit case calls that holding into question and indicates that the proper standard is “preponderance of the evidence.” Compare *Ridge Chrysler Jeep, LLC v. DaimlerChrysler Fin. Servs. Ams. LLC*, 516 F.3d 623, 625 (7th Cir. 2008) (stating that although a 2003 Seventh Circuit case, *Maynard*, used the “clear and convincing” standard, that case failed to discuss Supreme Court precedent holding “that heightened burdens of proof do not apply in civil cases unless a statute or the Constitution so requires”), with *Maynard v. Nygren*, 332 F.3d 462, 468 (7th Cir. 2003) (court must have “clear and convincing evidence of

willfulness, bad faith or fault before dismissing a case"); see also *Grogan v. Garner*, 498 U.S. 279 (1991); *Herman & MacLean v. Huddleston*, 459 U.S. 375 (1983).

B. Present Case

After reviewing the pertinent standards and the record currently before the Court, UIC has not shown that it is entitled to sanctions, including the entry of a judgment in its favor. In particular, (1) there is insufficient evidence that Grubb had control over the laptop in question when it was wiped by ABO; (2) the circumstances associated with handing over the laptop do not support an inference of bad faith; (3) there is no evidence that Grubb knew or suspected *ex ante* that ABO would wipe the machine and destroy data; (4) there is no evidence that there were usable data on the computer when it was wiped, and (5) the only evidence indicates that there were no usable data at the time that Grubb was advised to stop using the computer.

As to the first three points, there is a true evidentiary gap. The deposition testimony of Grubb suggests that he learned of the laptop's fate only after he returned it to ABO. See Grubb Dep. at 176. Moreover, the evidence indicates that ABO was conducting some sort of investigation into the July 18 incident as well. The factual picture surrounding the decision to hand the laptop over to ABO is unclear, but there is no indication that it was unreasonable to return ABO's property, particularly as counsel for ABO had indicated that they might be conducting some sort of forensic analysis on the computer.² The subsequent destruction of the laptop data was carried out by ABO rather than Grubb, who learned of the circumstances one week prior to his deposition. See Grubb Dep. at 177. There is simply too little evidence in the

² The record does not disclose whether such an investigation still was intended at the time when the laptop was actually returned.

record to support a finding of bad faith on the part of Grubb with respect to the decision to destroy the laptop.

Of course, the actual destruction of the laptop might be of only academic importance anyway. The final two shortcomings—the lack of evidence that there were usable data on the computer when it was wiped, and the evidence indicating that there were no usable data at the time Grubb was advised to stop using the computer—prove more important. As UIC acknowledges in its brief, at the time that the Sidley Austin lawyer issued her warning, ABO’s computer expert told Grubb that there were no usable data on the laptop. One month elapsed from the time of the July 18 incident to the August 18 e-mail from the Sidley Austin lawyer. The only person who advised Grubb that appeared to have pertinent personal knowledge (the frequency of Grubb’s use of the laptop) indicated that there were no usable data on the laptop. Any destruction of evidence thus occurred before it can be said that Grubb knew or should have known that workaday use could have an impact on the evidentiary value of the laptop. UIC has offered no evidence to the contrary. And when it comes to the forensic trail on a computer hard drive, it cannot be said that everyday people would possess an understanding of how data are stored and how access history can be reconstructed (or destroyed). That certainly cannot be said of Grubb, who indicated that he knew how to turn his laptop on but knew little else about how computers work. Thus, the evidence does not support the conclusion that Grubb took his actions for the purpose of hiding adverse information. *Mathis*, 136 F.3d at 1155. And although UIC brings its motion pursuant to the Court’s inherent authority, the Court is mindful of Federal Rule of Civil Procedure 37(e), which provides that “[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information

system.” The Supreme Court has warned that inherent powers “must be exercised with restraint and discretion” (*Chambers v. NASCO, Inc.*, 501 U.S. 32, 44 (1991)), and restraint seems eminently sensible given the content of the federal rules.

In sum, under the governing legal standards, UIC has not established that sanctionable conduct occurred in this case. That conclusion is reinforced by the Seventh Circuit’s critical teaching that sanctions for destruction of evidence should be proportional to the wrong. *E.g.*, *Collins*, 554 F.3d at 698. An application of that teaching is that destruction of evidence that has limited probative value (or is cumulative to the moving party’s case) does not warrant dismissal. In that regard, the parties’ briefing and the record before the Court indicate that Grubb may have a weak case. Grubb indicated in his deposition testimony that he does not know if UIC accessed data or removed anything other than the UIC software, and he indicated that the computer worked fine after the incident. Under the CFAA’s provision that creates a cause of action, a person can, as a general matter, recover for either “damage” or “loss” as defined in the statute. However, in order to recover for either damage or loss, a person must show that the defendant violated the CFAA’s proscriptive provisions. Grubb has not identified the statutory hook to which he hitches his cause of action, but it appears that one of two provisions may apply: under 18 U.S.C. §§ 1030(a)(5)(A) and (a)(5)(B) a person may be liable if he engages in unauthorized access and either (1) recklessly causes damage or (2) merely causes (no state-of-mind requirement) damages *and* loss.

Therefore, under the theories that Grubb likely is pursuing, he will have to show “damage” as defined in the statute. But “damage” is defined in § 1030(e) to mean “any impairment to the integrity or availability of data, a program, a system, or information.” Grubb may take the position that he takes in his deposition—that integrity just means that data is

compromised because someone may have laid eyes on it—but that panoptic definition cannot be right, because the argument conflates “access” with “damage.” The statute cannot bear the construction because its plain language requires *both* access *and* damage before liability may be imposed. *E.g.*, 18 U.S.C. § 1030(a)(5)(B) (imposing liability on one who “intentionally accesses a protected computer without authorization, *and* as a result of such conduct, recklessly causes damage” (emphasis added)). Given that damage *and* access have distinct meanings under the statute, the following exchange during Grubb’s deposition may prove important—and fatal:

Q. Did you ever ask anyone to check your hard drive to see if it worked after [the July 18 incident]?

A. To see if it worked?

Q. Yes.

A. Yes, the computer worked.

* * *

A. Yes, the computer worked fine.

Q. Did you ask anyone to check any other functions on your computer to see if they worked after the UIC accessed the computer?

A. The computer worked fine. The reason that I was getting a new one was because * * * we needed a much faster and much larger memory * * *.

Q. Did you yourself examine any other programs or systems or data on the computer to see if they worked?

A. Everything worked fine on the computer.

* * *

Q. Did you ever ask anyone to determine whether any program or data had been impaired in any way?

A. No, I wouldn't ask anybody something like that unless I noticed material or a program was impaired and then I would have asked them.

Grubb Dep. 183-84. If (a) no one ever examined the computer in order to see if damage had occurred, (b) Grubb never noticed that there were any problems with the computer, and (c) Grubb cannot show that any data on the computer were accessed, then Grubb would appear to have, putting it mildly, a serious evidence problem. See also Grubb Dep. at 203-04 (indicating that no data was destroyed or impaired and that the computer was "fully operable"). That dearth of evidence cuts both ways: because his case is weak and any evidence that was left on the machine at the time it was destroyed would have been difficult to glean, sanctions are not warranted. However, that same dearth of evidence may doom Grubb's case.

III. Conclusion

For the reasons set forth above, UIC's motion for sanctions for spoliation of evidence [14] is denied. However, this order does not address the wisdom of either side deploying the heavy artillery of federal litigation in pursuing this matter. Grubb's deposition testimony makes the presence of "damage" or "loss," as defined by the CFAA, rather doubtful. And even if damage occurred, Grubb's estimate of loss in the amount of nearly \$1 million would appear dead on arrival. Under the statute, one can recover losses only for costs associated with interruption of service. But Grubb stated in his deposition that he suffered no interruption of service. Grubb Dep. at 204. In these circumstances, both parties should consider whether—in a case in which the prevailing party's bill of costs may well exceed any plausible award of damages—the vindication game is worth the litigation candle.

A handwritten signature in black ink, appearing to read "Robert M. Dow, Jr."

Dated: August 4, 2010

Robert M. Dow, Jr.
United States District Judge